

(2) FORM OF REPORT.—

(A) IN GENERAL.—Each report required by paragraph (1) shall be submitted in unclassified form but may include a classified annex.

(B) PUBLIC AVAILABILITY.—The Secretary of the Treasury shall post the unclassified portion of each report required by paragraph (1) on a publicly available internet website of the Department of the Treasury.

(b) IMPOSITION OF SANCTIONS.—The Secretary of the Treasury may prohibit the opening, or prohibit or impose strict conditions on the maintaining, in the United States of a correspondent account or a payable-through account by a foreign financial institution identified under subsection (a)(1).

SEC. 1296. EXCEPTIONS; WAIVERS; IMPLEMENTATION.

(a) EXCEPTIONS.—

(1) EXCEPTION FOR INTELLIGENCE, LAW ENFORCEMENT, AND NATIONAL SECURITY ACTIVITIES.—Sanctions under sections 1294 and 1295 shall not apply to any authorized intelligence, law enforcement, or national security activities of the United States.

(2) EXCEPTION TO COMPLY WITH UNITED NATIONS HEADQUARTERS AGREEMENT.—Sanctions under section 1294(c)(2) shall not apply with respect to the admission of an alien to the United States if the admission of the alien is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, the Convention on Consular Relations, done at Vienna April 24, 1963, and entered into force March 19, 1967, or other applicable international obligations.

(3) EXCEPTION RELATING TO IMPORTATION OF GOODS.—

(A) IN GENERAL.—Notwithstanding any other provision of this subtitle, the authorities and requirements to impose sanctions authorized under this subtitle shall not include the authority or a requirement to impose sanctions on the importation of goods.

(B) GOOD DEFINED.—In this paragraph, the term “good” means any article, natural or manmade substance, material, supply or manufactured product, including inspection and test equipment, and excluding technical data.

(b) NATIONAL SECURITY WAIVER.—The President may waive the application of sanctions under section 1294 with respect to a person if the President—

(1) determines that the waiver is in the national security interests of the United States; and

(2) submits to the appropriate congressional committees a report on the waiver and the reasons for the waiver.

(c) IMPLEMENTATION; PENALTIES.—

(1) IMPLEMENTATION.—The President may exercise all authorities provided to the President under sections 203 and 205 of the International Emergency Economic Powers Act (50 U.S.C. 1702 and 1704) to carry out this subtitle.

(2) PENALTIES.—A person that violates, attempts to violate, conspires to violate, or causes a violation of section 1294(b)(1) or 1295(b) or any regulation, license, or order issued to carry out either such section shall be subject to the penalties set forth in subsections (b) and (c) of section 206 of the International Emergency Economic Powers Act (50 U.S.C. 1705) to the same extent as a person that commits an unlawful act described in subsection (a) of that section.

SA 4670. Mr. BARRASSO submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed

to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title XII, add the following:

SEC. 1283. REMOVAL OF MEMBERS OF THE UNITED NATIONS HUMAN RIGHTS COUNCIL THAT COMMIT HUMAN RIGHTS ABUSES.

The President shall direct the Permanent Representative of the United States to the United Nations to use the voice, vote, and influence of the United States—

(1) to reform the process for removing members of the United Nations Human Rights Council that commit gross and systemic violations of human rights, including—

(A) lowering the threshold vote at the United Nations General Assembly for removal to a simple majority;

(B) ensuring that information detailing the member country's human rights record is publicly available before the vote on removal; and

(C) making the vote of each country on the removal from the United Nations Human Rights Council publicly available;

(2) to reform the rules on electing members to the United Nations Human Rights Council to ensure that United Nations members which have committed gross and systemic violations of human rights are not elected to the Human Rights Council; and

(3) to oppose the election to the Human Rights Council of any United Nations member—

(A) that is currently designated as—

(i) a country engaged in a consistent pattern of gross violations of internationally recognized human rights pursuant to section 116 or section 502B of the Foreign Assistance Act of 1961 (22 U.S.C. 2151n and 2304);

(ii) a state sponsor of terrorism; or

(iii) a Tier 3 country under the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7101 et seq.);

(B) the government of which is identified on the list published by the Secretary of State pursuant to section 404(b) of the Child Soldiers Prevention Act of 2008 (22 U.S.C. 2370c–1(b)) as a government that recruits and uses child soldiers; or

(C) the government of which the United States determines to have committed genocide or crimes against humanity.

SA 4671. Mr. TOOMEY (for himself and Mr. CASEY) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle D of title II, add the following:

SEC. 246. BRIEFING ON ADDITIVE MANUFACTURING CAPABILITIES.

(a) IN GENERAL.—Not later than 90 days after the date of the enactment of this Act, the Director of the Army Combat Capabili-

ties Development Command shall brief the congressional defense committees on—

(1) current research and development activities to leverage robotics, autonomy, and artificial intelligence to enhance additive manufacturing capabilities in forward-deployed, expeditionary bases; and

(2) courses of action being considered to successfully transition additive manufacturing capabilities into sustained operational capabilities.

(b) ELEMENTS.—The briefing required by subsection (a) shall include the following:

(1) A summary of research advances and innovations in expeditionary manufacturing enabled by past investments combining artificial intelligence and additive manufacturing.

(2) A summary of plans and ongoing activities to engage with operational programs and programs of record to ensure that such advances and innovations can be successfully transitioned and supported to maximize mission readiness and force resiliency.

(3) An assessment of the feasibility of initiating pilot programs between institutions of higher education, the defense industrial base, and the Army Combat Capabilities Development Command related to experimentation and demonstrations of expeditionary manufacturing techniques.

SA 4672. Mr. KENNEDY submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1064. SYSTEM FOR ELECTRONIC SUBMISSION OF COMPLAINTS ABOUT THE DELIVERY OF HEALTH CARE SERVICES BY THE DEPARTMENT OF VETERANS AFFAIRS.

Section 7309A(c) of title 38, United States Code, is amended by adding at the end the following new paragraph:

“(3) Beginning not later than 18 months after the date of the enactment of this paragraph, the Director shall establish an information technology system that will allow a veteran (or the designated representative of a veteran) to electronically—

“(A) file a complaint that will be received by the appropriate patient advocate; and

“(B) at any time view the status of the complaint, including interim and final actions that have been taken to address the complaint.”.

SA 4673. Mr. PETERS (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—CYBER INCIDENT REPORTING ACT OF 2021 AND CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

TITLE LI—CYBER INCIDENT REPORTING ACT OF 2021

SEC. 5101. SHORT TITLE.

This title may be cited as the “Cyber Incident Reporting Act of 2021”.

SEC. 5102. DEFINITIONS.

In this title:

(1) **COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT.**—The terms “covered cyber incident”, “covered entity”, and “cyber incident” have the meanings given those terms in section 2230 of the Homeland Security Act of 2002, as added by section 5103 of this title.

(2) **DIRECTOR.**—The term “Director” means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) **INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.**—The terms “information system”, “ransom payment”, “ransomware attack”, and “security vulnerability” have the meanings given those terms in section 2200 of the Homeland Security Act of 2002, as added by section 5203 of this division.

SEC. 5103. CYBER INCIDENT REPORTING.

(a) **CYBER INCIDENT REPORTING.**—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) in section 2209(b) (6 U.S.C. 659(b)), as so redesignated by section 5203(b) of this division—

(A) in paragraph (11), by striking “and” at the end;

(B) in paragraph (12), by striking the period at the end and inserting “; and”; and

(C) by adding at the end the following:

“(13) receiving, aggregating, and analyzing reports related to covered cyber incidents (as defined in section 2230) submitted by covered entities (as defined in section 2230) and reports related to ransom payments submitted by entities in furtherance of the activities specified in sections 2202(e), 2203, and 2231, this subsection, and any other authorized activity of the Director, to enhance the situational awareness of cybersecurity threats across critical infrastructure sectors.”; and

(2) by adding at the end the following:

“Subtitle C—Cyber Incident Reporting

“SEC. 2230. DEFINITIONS.

“In this subtitle:

“(1) **CENTER.**—The term ‘Center’ means the center established under section 2209.

“(2) **COUNCIL.**—The term ‘Council’ means the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)).

“(3) **COVERED CYBER INCIDENT.**—The term ‘covered cyber incident’ means a substantial cyber incident experienced by a covered entity that satisfies the definition and criteria established by the Director in the final rule issued pursuant to section 2232(b).

“(4) **COVERED ENTITY.**—The term ‘covered entity’ means—

“(A) any Federal contractor; or

“(B) an entity that owns or operates critical infrastructure that satisfies the definition established by the Director in the final rule issued pursuant to section 2232(b).

“(5) **CYBER INCIDENT.**—The term ‘cyber incident’ has the meaning given the term ‘incident’ in section 2200.

“(6) **CYBER THREAT.**—The term ‘cyber threat’—

“(A) has the meaning given the term ‘cybersecurity threat’ in section 2200; and

“(B) does not include any activity related to good faith security research, including

participation in a bug-bounty program or a vulnerability disclosure program.

“(7) **FEDERAL CONTRACTOR.**—The term ‘Federal contractor’ means a business, nonprofit organization, or other private sector entity that holds a Federal Government contract or subcontract at any tier, grant, cooperative agreement, or other transaction agreement, unless that entity is a party only to—

“(A) a service contract to provide housekeeping or custodial services; or

“(B) a contract to provide products or services unrelated to information technology that is below the micro-purchase threshold, as defined in section 2.101 of title 48, Code of Federal Regulations, or any successor regulation.

“(8) **FEDERAL ENTITY; INFORMATION SYSTEM; SECURITY CONTROL.**—The terms ‘Federal entity’, ‘information system’, and ‘security control’ have the meanings given those terms in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

“(9) **SIGNIFICANT CYBER INCIDENT.**—The term ‘significant cyber incident’ means a cybersecurity incident, or a group of related cybersecurity incidents, that the Secretary determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the people of the United States.

“(10) **SMALL ORGANIZATION.**—The term ‘small organization’—

“(A) means—

“(i) a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632); or

“(ii) any nonprofit organization, including faith-based organizations and houses of worship, or other private sector entity with fewer than 200 employees (determined on a full-time equivalent basis); and

“(B) does not include—

“(i) a business, nonprofit organization, or other private sector entity that is a covered entity; or

“(ii) a Federal contractor.

“SEC. 2231. CYBER INCIDENT REVIEW.

“(a) **ACTIVITIES.**—The Center shall—

“(1) receive, aggregate, analyze, and secure, using processes consistent with the processes developed pursuant to the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) reports from covered entities related to a covered cyber incident to assess the effectiveness of security controls, identify tactics, techniques, and procedures adversaries use to overcome those controls and other cybersecurity purposes, including to support law enforcement investigations, to assess potential impact of incidents on public health and safety, and to have a more accurate picture of the cyber threat to critical infrastructure and the people of the United States;

“(2) receive, aggregate, analyze, and secure reports to lead the identification of tactics, techniques, and procedures used to perpetuate cyber incidents and ransomware attacks;

“(3) coordinate and share information with appropriate Federal departments and agencies to identify and track ransom payments, including those utilizing virtual currencies;

“(4) leverage information gathered about cybersecurity incidents to—

“(A) enhance the quality and effectiveness of information sharing and coordination efforts with appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, critical infrastructure owners and operators, cybersecurity and incident response firms, and security researchers; and

“(B) provide appropriate entities, including agencies, sector coordinating councils, information sharing and analysis organizations, technology providers, cybersecurity and incident response firms, and security researchers, with timely, actionable, and anonymized reports of cyber incident campaigns and trends, including, to the maximum extent practicable, related contextual information, cyber threat indicators, and defensive measures, pursuant to section 2235;

“(5) establish mechanisms to receive feedback from stakeholders on how the Agency can most effectively receive covered cyber incident reports, ransom payment reports, and other voluntarily provided information;

“(6) facilitate the timely sharing, on a voluntary basis, between relevant critical infrastructure owners and operators of information relating to covered cyber incidents and ransom payments, particularly with respect to ongoing cyber threats or security vulnerabilities and identify and disseminate ways to prevent or mitigate similar incidents in the future;

“(7) for a covered cyber incident, including a ransomware attack, that also satisfies the definition of a significant cyber incident, or is part of a group of related cyber incidents that together satisfy such definition, conduct a review of the details surrounding the covered cyber incident or group of those incidents and identify and disseminate ways to prevent or mitigate similar incidents in the future;

“(8) with respect to covered cyber incident reports under section 2232(a) and 2233 involving an ongoing cyber threat or security vulnerability, immediately review those reports for cyber threat indicators that can be anonymized and disseminated, with defensive measures, to appropriate stakeholders, in coordination with other divisions within the Agency, as appropriate;

“(9) publish quarterly unclassified, public reports that may be based on the unclassified information contained in the briefings required under subsection (c);

“(10) proactively identify opportunities and perform analyses, consistent with the protections in section 2235, to leverage and utilize data on ransomware attacks to support law enforcement operations to identify, track, and seize ransom payments utilizing virtual currencies, to the greatest extent practicable;

“(11) proactively identify opportunities, consistent with the protections in section 2235, to leverage and utilize data on cyber incidents in a manner that enables and strengthens cybersecurity research carried out by academic institutions and other private sector organizations, to the greatest extent practicable;

“(12) on a not less frequently than annual basis, analyze public disclosures made pursuant to parts 229 and 249 of title 17, Code of Federal Regulations, or any subsequent document submitted to the Securities and Exchange Commission by entities experiencing cyber incidents and compare such disclosures to reports received by the Center; and

“(13) in accordance with section 2235 and subsection (b) of this section, as soon as possible but not later than 24 hours after receiving a covered cyber incident report, ransom payment report, voluntarily submitted information pursuant to section 2233, or information received pursuant to a request for information or subpoena under section 2234, make available the information to appropriate Sector Risk Management Agencies and other appropriate Federal agencies.

“(b) **INTERAGENCY SHARING.**—The National Cyber Director, in consultation with the Director and the Director of the Office of Management and Budget—

“(1) may establish a specific time requirement for sharing information under subsection (a)(13); and

“(2) shall determine the appropriate Federal agencies under subsection (a)(13).

“(c) PERIODIC BRIEFING.—Not later than 60 days after the effective date of the final rule required under section 2232(b), and on the first day of each month thereafter, the Director, in consultation with the National Cyber Director, the Attorney General, and the Director of National Intelligence, shall provide to the majority leader of the Senate, the minority leader of the Senate, the Speaker of the House of Representatives, the minority leader of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Homeland Security of the House of Representatives a briefing that characterizes the national cyber threat landscape, including the threat facing Federal agencies and covered entities, and applicable intelligence and law enforcement information, covered cyber incidents, and ransomware attacks, as of the date of the briefing, which shall—

“(1) include the total number of reports submitted under sections 2232 and 2233 during the preceding month, including a breakdown of required and voluntary reports;

“(2) include any identified trends in covered cyber incidents and ransomware attacks over the course of the preceding month and as compared to previous reports, including any trends related to the information collected in the reports submitted under sections 2232 and 2233, including—

“(A) the infrastructure, tactics, and techniques malicious cyber actors commonly use; and

“(B) intelligence gaps that have impeded, or currently are impeding, the ability to counter covered cyber incidents and ransomware threats;

“(3) include a summary of the known uses of the information in reports submitted under sections 2232 and 2233; and

“(4) be unclassified, but may include a classified annex.

“SEC. 2232. REQUIRED REPORTING OF CERTAIN CYBER INCIDENTS.

“(a) IN GENERAL.—

“(1) COVERED CYBER INCIDENT REPORTS.—A covered entity that is a victim of a covered cyber incident shall report the covered cyber incident to the Director not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.

“(2) RANSOM PAYMENT REPORTS.—An entity, including a covered entity and except for an individual or a small organization, that makes a ransom payment as the result of a ransomware attack against the entity shall report the payment to the Director not later than 24 hours after the ransom payment has been made.

“(3) SUPPLEMENTAL REPORTS.—A covered entity shall promptly submit to the Director an update or supplement to a previously submitted covered cyber incident report if new or different information becomes available or if the covered entity makes a ransom payment after submitting a covered cyber incident report required under paragraph (1).

“(4) PRESERVATION OF INFORMATION.—Any entity subject to requirements of paragraph (1), (2), or (3) shall preserve data relevant to the covered cyber incident or ransom payment in accordance with procedures established in the final rule issued pursuant to subsection (b).

“(5) EXCEPTIONS.—

“(A) REPORTING OF COVERED CYBER INCIDENT WITH RANSOM PAYMENT.—If a covered cyber incident includes a ransom payment such that the reporting requirements under

paragraphs (1) and (2) apply, the covered entity may submit a single report to satisfy the requirements of both paragraphs in accordance with procedures established in the final rule issued pursuant to subsection (b).

“(B) SUBSTANTIALLY SIMILAR REPORTED INFORMATION.—The requirements under paragraphs (1), (2), and (3) shall not apply to an entity required by law, regulation, or contract to report substantially similar information to another Federal agency within a substantially similar timeframe.

“(C) DOMAIN NAME SYSTEM.—The requirements under paragraphs (1), (2) and (3) shall not apply to an entity or the functions of an entity that the Director determines constitute critical infrastructure owned, operated, or governed by multi-stakeholder organizations that develop, implement, and enforce policies concerning the Domain Name System, such as the Internet Corporation for Assigned Names and Numbers or the Internet Assigned Numbers Authority.

“(6) MANNER, TIMING, AND FORM OF REPORTS.—Reports made under paragraphs (1), (2), and (3) shall be made in the manner and form, and within the time period in the case of reports made under paragraph (3), prescribed in the final rule issued pursuant to subsection (b).

“(7) EFFECTIVE DATE.—Paragraphs (1) through (4) shall take effect on the dates prescribed in the final rule issued pursuant to subsection (b).

“(b) RULEMAKING.—

“(1) NOTICE OF PROPOSED RULEMAKING.—Not later than 2 years after the date of enactment of this section, the Director, in consultation with Sector Risk Management Agencies, the Department of Justice, and other Federal agencies, shall publish in the Federal Register a notice of proposed rulemaking to implement subsection (a).

“(2) FINAL RULE.—Not later than 18 months after publication of the notice of proposed rulemaking under paragraph (1), the Director shall issue a final rule to implement subsection (a).

“(3) SUBSEQUENT RULEMAKINGS.—

“(A) IN GENERAL.—The Director is authorized to issue regulations to amend or revise the final rule issued pursuant to paragraph (2).

“(B) PROCEDURES.—Any subsequent rules issued under subparagraph (A) shall comply with the requirements under chapter 5 of title 5, United States Code, including the issuance of a notice of proposed rulemaking under section 553 of such title.

“(c) ELEMENTS.—The final rule issued pursuant to subsection (b) shall be composed of the following elements:

“(1) A clear description of the types of entities that constitute covered entities, based on—

“(A) the consequences that disruption to or compromise of such an entity could cause to national security, economic security, or public health and safety;

“(B) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country; and

“(C) the extent to which damage, disruption, or unauthorized access to such an entity, including the accessing of sensitive cybersecurity vulnerability information or penetration testing tools or techniques, will likely enable the disruption of the reliable operation of critical infrastructure.

“(2) A clear description of the types of substantial cyber incidents that constitute covered cyber incidents, which shall—

“(A) at a minimum, require the occurrence of—

“(i) the unauthorized access to an information system or network with a substantial loss of confidentiality, integrity, or availability of such information system or net-

work, or a serious impact on the safety and resiliency of operational systems and processes;

“(ii) a disruption of business or industrial operations due to a cyber incident; or

“(iii) an occurrence described in clause (i) or (ii) due to loss of service facilitated through, or caused by, a compromise of a cloud service provider, managed service provider, or other third-party data hosting provider or by a supply chain compromise;

“(B) consider—

“(i) the sophistication or novelty of the tactics used to perpetrate such an incident, as well as the type, volume, and sensitivity of the data at issue;

“(ii) the number of individuals directly or indirectly affected or potentially affected by such an incident; and

“(iii) potential impacts on industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers; and

“(C) exclude—

“(i) any event where the cyber incident is perpetuated by good faith security research or in response to an invitation by the owner or operator of the information system for third parties to find vulnerabilities in the information system, such as through a vulnerability disclosure program or the use of authorized penetration testing services; and

“(ii) the threat of disruption as extortion, as described in section 2201(9)(A).

“(3) A requirement that, if a covered cyber incident or a ransom payment occurs following an exempted threat described in paragraph (2)(C)(ii), the entity shall comply with the requirements in this subtitle in reporting the covered cyber incident or ransom payment.

“(4) A clear description of the specific required contents of a report pursuant to subsection (a)(1), which shall include the following information, to the extent applicable and available, with respect to a covered cyber incident:

“(A) A description of the covered cyber incident, including—

“(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such incident;

“(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

“(iii) the estimated date range of such incident; and

“(iv) the impact to the operations of the covered entity.

“(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the covered cyber incident.

“(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such incident.

“(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person.

“(E) The name and other information that clearly identifies the entity impacted by the covered cyber incident.

“(F) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the covered entity or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, the covered entity to assist

with compliance with the requirements of this subtitle.

“(5) A clear description of the specific required contents of a report pursuant to subsection (a)(2), which shall be the following information, to the extent applicable and available, with respect to a ransom payment:

“(A) A description of the ransomware attack, including the estimated date range of the attack.

“(B) Where applicable, a description of the vulnerabilities, tactics, techniques, and procedures used to perpetuate the ransomware attack.

“(C) Where applicable, any identifying or contact information related to the actor or actors reasonably believed to be responsible for the ransomware attack.

“(D) The name and other information that clearly identifies the entity that made the ransom payment.

“(E) Contact information, such as telephone number or electronic mail address, that the Center may use to contact the entity that made the ransom payment or an authorized agent of such covered entity, or, where applicable, the service provider of such covered entity acting with the express permission of, and at the direction of, that entity to assist with compliance with the requirements of this subtitle.

“(F) The date of the ransom payment.

“(G) The ransom payment demand, including the type of virtual currency or other commodity requested, if applicable.

“(H) The ransom payment instructions, including information regarding where to send the payment, such as the virtual currency address or physical address the funds were requested to be sent to, if applicable.

“(I) The amount of the ransom payment.

“(6) A clear description of the types of data required to be preserved pursuant to subsection (a)(4) and the period of time for which the data is required to be preserved.

“(7) Deadlines for submitting reports to the Director required under subsection (a)(3), which shall—

“(A) be established by the Director in consultation with the Council;

“(B) consider any existing regulatory reporting requirements similar in scope, purpose, and timing to the reporting requirements to which such a covered entity may also be subject, and make efforts to harmonize the timing and contents of any such reports to the maximum extent practicable; and

“(C) balance the need for situational awareness with the ability of the covered entity to conduct incident response and investigations.

“(8) Procedures for—

“(A) entities to submit reports required by paragraphs (1), (2), and (3) of subsection (a), including the manner and form thereof, which shall include, at a minimum, a concise, user-friendly web-based form;

“(B) the Agency to carry out the enforcement provisions of section 2233, including with respect to the issuance, service, withdrawal, and enforcement of subpoenas, appeals and due process procedures, the suspension and debarment provisions in section 2234(c), and other aspects of noncompliance;

“(C) implementing the exceptions provided in subsection (a)(5); and

“(D) protecting privacy and civil liberties consistent with processes adopted pursuant to section 105(b) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(b)) and anonymizing and safeguarding, or no longer retaining, information received and disclosed through covered cyber incident reports and ransom payment reports that is known to be personal information of a specific individual or information that identifies a specific individual

that is not directly related to a cybersecurity threat.

“(9) A clear description of the types of entities that constitute other private sector entities for purposes of section 2230(b)(7).

“(d) **THIRD PARTY REPORT SUBMISSION AND RANSOM PAYMENT.**—

“(1) **REPORT SUBMISSION.**—An entity, including a covered entity, that is required to submit a covered cyber incident report or a ransom payment report may use a third party, such as an incident response company, insurance provider, service provider, information sharing and analysis organization, or law firm, to submit the required report under subsection (a).

“(2) **RANSOM PAYMENT.**—If an entity impacted by a ransomware attack uses a third party to make a ransom payment, the third party shall not be required to submit a ransom payment report for itself under subsection (a)(2).

“(3) **DUTY TO REPORT.**—Third-party reporting under this subparagraph does not relieve a covered entity or an entity that makes a ransom payment from the duty to comply with the requirements for covered cyber incident report or ransom payment report submission.

“(4) **RESPONSIBILITY TO ADVISE.**—Any third party used by an entity that knowingly makes a ransom payment on behalf of an entity impacted by a ransomware attack shall advise the impacted entity of the responsibilities of the impacted entity regarding reporting ransom payments under this section.

“(e) **OUTREACH TO COVERED ENTITIES.**—

“(1) **IN GENERAL.**—The Director shall conduct an outreach and education campaign to inform likely covered entities, entities that offer or advertise as a service to customers to make or facilitate ransom payments on behalf of entities impacted by ransomware attacks, potential ransomware attack victims, and other appropriate entities of the requirements of paragraphs (1), (2), and (3) of subsection (a).

“(2) **ELEMENTS.**—The outreach and education campaign under paragraph (1) shall include the following:

“(A) An overview of the final rule issued pursuant to subsection (b).

“(B) An overview of mechanisms to submit to the Center covered cyber incident reports and information relating to the disclosure, retention, and use of incident reports under this section.

“(C) An overview of the protections afforded to covered entities for complying with the requirements under paragraphs (1), (2), and (3) of subsection (a).

“(D) An overview of the steps taken under section 2234 when a covered entity is not in compliance with the reporting requirements under subsection (a).

“(E) Specific outreach to cybersecurity vendors, incident response providers, cybersecurity insurance entities, and other entities that may support covered entities or ransomware attack victims.

“(F) An overview of the privacy and civil liberties requirements in this subtitle.

“(3) **COORDINATION.**—In conducting the outreach and education campaign required under paragraph (1), the Director may coordinate with—

“(A) the Critical Infrastructure Partnership Advisory Council established under section 871;

“(B) information sharing and analysis organizations;

“(C) trade associations;

“(D) information sharing and analysis centers;

“(E) sector coordinating councils; and

“(F) any other entity as determined appropriate by the Director.

“(f) **ORGANIZATION OF REPORTS.**—Notwithstanding chapter 35 of title 44, United States Code (commonly known as the ‘Paperwork Reduction Act’), the Director may request information within the scope of the final rule issued under subsection (b) by the alteration of existing questions or response fields and the reorganization and reformatting of the means by which covered cyber incident reports, ransom payment reports, and any voluntarily offered information is submitted to the Center.

“**SEC. 2233. VOLUNTARY REPORTING OF OTHER CYBER INCIDENTS.**

“(a) **IN GENERAL.**—Entities may voluntarily report incidents or ransom payments to the Director that are not required under paragraph (1), (2), or (3) of section 2232(a), but may enhance the situational awareness of cyber threats.

“(b) **VOLUNTARY PROVISION OF ADDITIONAL INFORMATION IN REQUIRED REPORTS.**—Entities may voluntarily include in reports required under paragraph (1), (2), or (3) of section 2232(a) information that is not required to be included, but may enhance the situational awareness of cyber threats.

“(c) **APPLICATION OF PROTECTIONS.**—The protections under section 2235 applicable to covered cyber incident reports shall apply in the same manner and to the same extent to reports and information submitted under subsections (a) and (b).

“**SEC. 2234. NONCOMPLIANCE WITH REQUIRED REPORTING.**

“(a) **PURPOSE.**—In the event that an entity that is required to submit a report under section 2232(a) fails to comply with the requirement to report, the Director may obtain information about the incident or ransom payment by engaging the entity directly to request information about the incident or ransom payment, and if the Director is unable to obtain information through such engagement, by issuing a subpoena to the entity, pursuant to subsection (c), to gather information sufficient to determine whether a covered cyber incident or ransom payment has occurred, and, if so, whether additional action is warranted pursuant to subsection (d).

“(b) **INITIAL REQUEST FOR INFORMATION.**—

“(1) **IN GENERAL.**—If the Director has reason to believe, whether through public reporting or other information in the possession of the Federal Government, including through analysis performed pursuant to paragraph (1) or (2) of section 2231(a), that an entity has experienced a covered cyber incident or made a ransom payment but failed to report such incident or payment to the Center within 72 hours in accordance with section 2232(a), the Director shall request additional information from the entity to confirm whether or not a covered cyber incident or ransom payment has occurred.

“(2) **TREATMENT.**—Information provided to the Center in response to a request under paragraph (1) shall be treated as if it was submitted through the reporting procedures established in section 2232.

“(c) **AUTHORITY TO ISSUE SUBPOENAS AND DEBAR.**—

“(1) **IN GENERAL.**—If, after the date that is 72 hours from the date on which the Director made the request for information in subsection (b), the Director has received no response from the entity from which such information was requested, or received an inadequate response, the Director may issue to such entity a subpoena to compel disclosure of information the Director deems necessary to determine whether a covered cyber incident or ransom payment has occurred and obtain the information required to be reported pursuant to section 2232 and any implementing regulations.

“(2) CIVIL ACTION.—

“(A) IN GENERAL.—If an entity fails to comply with a subpoena, the Director may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena.

“(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the entity against which the action is brought resides, is found, or does business.

“(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this subsection as contempt of court.

“(3) NON-DELEGATION.—The authority of the Director to issue a subpoena under this subsection may not be delegated.

“(4) DEBARMENT OF FEDERAL CONTRACTORS.—If a covered entity that is a Federal contractor fails to comply with a subpoena issued under this subsection—

“(A) the Director may refer the matter to the Administrator of General Services; and

“(B) upon receiving a referral from the Director, the Administrator of General Services may impose additional available penalties, including suspension or debarment.

“(5) AUTHENTICATION.—

“(A) IN GENERAL.—Any subpoena issued electronically pursuant to this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

“(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of such subpoena.

“(d) ACTIONS BY ATTORNEY GENERAL AND FEDERAL REGULATORY AGENCIES.—

“(1) IN GENERAL.—Notwithstanding section 2235(a) and subsection (b)(2) of this section, if the Attorney General or the appropriate Federal regulatory agency determines, based on information provided in response to a subpoena issued pursuant to subsection (c), that the facts relating to the covered cyber incident or ransom payment at issue may constitute grounds for a regulatory enforcement action or criminal prosecution, the Attorney General or the appropriate Federal regulatory agency may use that information for a regulatory enforcement action or criminal prosecution.

“(2) APPLICATION TO CERTAIN ENTITIES AND THIRD PARTIES.—A covered cyber incident or ransom payment report submitted to the Center by an entity that makes a ransom payment or third party under section 2232 shall not be used by any Federal, State, Tribal, or local government to investigate or take another law enforcement action against the entity that makes a ransom payment or third party.

“(3) RULE OF CONSTRUCTION.—Nothing in this subtitle shall be construed to provide an entity that submits a covered cyber incident report or ransom payment report under section 2232 any immunity from law enforcement action for making a ransom payment otherwise prohibited by law.

“(e) CONSIDERATIONS.—When determining whether to exercise the authorities provided under this section, the Director shall take into consideration—

“(1) the size and complexity of the entity;

“(2) the complexity in determining if a covered cyber incident has occurred; and

“(3) prior interaction with the Agency or awareness of the entity of the policies and procedures of the Agency for reporting covered cyber incidents and ransom payments.

“(f) EXCLUSIONS.—This section shall not apply to a State, local, Tribal, or territorial government entity.

“(g) REPORT TO CONGRESS.—The Director shall submit to Congress an annual report on the number of times the Director—

“(1) issued an initial request for information pursuant to subsection (b);

“(2) issued a subpoena pursuant to subsection (c); or

“(3) referred a matter to the Attorney General for a civil action pursuant to subsection (c)(2).

“(h) PUBLICATION OF THE ANNUAL REPORT.—The Director shall publish a version of the annual report required under subsection (g) on the website of the Agency, which shall include, at a minimum, the number of times the Director—

“(1) issued an initial request for information pursuant to subsection (b); or

“(2) issued a subpoena pursuant to subsection (c).

“(i) ANONYMIZATION OF REPORTS.—The Director shall ensure any victim information contained in a report required to be published under subsection (h) be anonymized before the report is published.

“SEC. 2235. INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

“(a) DISCLOSURE, RETENTION, AND USE.—

“(1) AUTHORIZED ACTIVITIES.—Information provided to the Center or Agency pursuant to section 2232 or 2233 may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

“(A) a cybersecurity purpose;

“(B) the purpose of identifying—

“(i) a cyber threat, including the source of the cyber threat; or

“(ii) a security vulnerability;

“(C) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a terrorist act or use of a weapon of mass destruction;

“(D) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

“(E) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a cyber incident reported pursuant to section 2232 or 2233 or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

“(2) AGENCY ACTIONS AFTER RECEIPT.—

“(A) RAPID, CONFIDENTIAL SHARING OF CYBER THREAT INDICATORS.—Upon receiving a covered cyber incident or ransom payment report submitted pursuant to this section, the center shall immediately review the report to determine whether the incident that is the subject of the report is connected to an ongoing cyber threat or security vulnerability and where applicable, use such report to identify, develop, and rapidly disseminate to appropriate stakeholders actionable, anonymized cyber threat indicators and defensive measures.

“(B) STANDARDS FOR SHARING SECURITY VULNERABILITIES.—With respect to information in a covered cyber incident or ransom payment report regarding a security vulnerability referred to in paragraph (1)(B)(ii), the Director shall develop principles that govern the timing and manner in which information relating to security vulnerabilities may be shared, consistent with common industry best practices and United States and international standards.

“(3) PRIVACY AND CIVIL LIBERTIES.—Information contained in covered cyber incident and ransom payment reports submitted to the Center or the Agency pursuant to section 2232 shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in accordance with processes to be developed for the protection of personal information consistent with processes adopted pursuant to section 105 of the Cybersecurity Act of 2015 (6 U.S.C. 1504) and in a manner that protects from unauthorized use or disclosure any information that may contain—

“(A) personal information of a specific individual; or

“(B) information that identifies a specific individual that is not directly related to a cybersecurity threat.

“(4) DIGITAL SECURITY.—The Center and the Agency shall ensure that reports submitted to the Center or the Agency pursuant to section 2232, and any information contained in those reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document.

“(5) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—A Federal, State, local, or Tribal government shall not use information about a covered cyber incident or ransom payment obtained solely through reporting directly to the Center or the Agency in accordance with this subtitle to regulate, including through an enforcement action, the activities of the covered entity or entity that made a ransom payment.

“(b) NO WAIVER OF PRIVILEGE OR PROTECTION.—The submission of a report to the Center or the Agency under section 2232 shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection and attorney-client privilege.

“(c) EXEMPTION FROM DISCLOSURE.—Information contained in a report submitted to the Office under section 2232 shall be exempt from disclosure under section 552(b)(3)(B) of title 5, United States Code (commonly known as the ‘Freedom of Information Act’) and any State, Tribal, or local provision of law requiring disclosure of information or records.

“(d) EX PARTE COMMUNICATIONS.—The submission of a report to the Agency under section 2232 shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decision-making official.

“(e) LIABILITY PROTECTIONS.—

“(1) IN GENERAL.—No cause of action shall lie or be maintained in any court by any person or entity and any such action shall be promptly dismissed for the submission of a report pursuant to section 2232(a) that is submitted in conformance with this subtitle and the rule promulgated under section 2232(b), except that this subsection shall not apply with regard to an action by the Federal Government pursuant to section 2234(c)(2).

“(2) SCOPE.—The liability protections provided in subsection (e) shall only apply to or affect litigation that is solely based on the submission of a covered cyber incident report or ransom payment report to the Center or the Agency.

“(3) RESTRICTIONS.—Notwithstanding paragraph (2), no report submitted to the Agency pursuant to this subtitle or any communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such report, may be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United

States, a State, or a political subdivision thereof, provided that nothing in this subtitle shall create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting such report.

“(f) **SHARING WITH NON-FEDERAL ENTITIES.**—The Agency shall anonymize the victim who reported the information when making information provided in reports received under section 2232 available to critical infrastructure owners and operators and the general public.

“(g) **PROPRIETARY INFORMATION.**—Information contained in a report submitted to the Agency under section 2232 shall be considered the commercial, financial, and proprietary information of the covered entity when so designated by the covered entity.

“(h) **STORED COMMUNICATIONS ACT.**—Nothing in this subtitle shall be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the ‘Stored Communications Act’).”.

(b) **TECHNICAL AND CONFORMING AMENDMENT.**—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the items relating to subtitle B of title XXII the following:

“Subtitle C—Cyber Incident Reporting
 “Sec. 2230. Definitions.
 “Sec. 2231. Cyber Incident Review.
 “Sec. 2232. Required reporting of certain cyber incidents.
 “Sec. 2233. Voluntary reporting of other cyber incidents.
 “Sec. 2234. Noncompliance with required reporting.
 “Sec. 2235. Information shared with or provided to the Federal Government.”.

SEC. 5104. FEDERAL SHARING OF INCIDENT REPORTS.

(a) **CYBER INCIDENT REPORTING SHARING.**—
 (1) **IN GENERAL.**—Notwithstanding any other provision of law or regulation, any Federal agency, including any independent establishment (as defined in section 104 of title 5, United States Code), that receives a report from an entity of a cyber incident, including a ransomware attack, shall provide the report to the Director as soon as possible, but not later than 24 hours after receiving the report, unless a shorter period is required by an agreement made between the Cybersecurity Infrastructure Security Agency and the recipient Federal agency. The Director shall share and coordinate each report pursuant to section 2231(b) of the Homeland Security Act of 2002, as added by section 5103 of this title.

(2) **RULE OF CONSTRUCTION.**—The requirements described in paragraph (1) shall not be construed to be a violation of any provision of law or policy that would otherwise prohibit disclosure within the executive branch.

(3) **PROTECTION OF INFORMATION.**—The Director shall comply with any obligations of the recipient Federal agency described in paragraph (1) to protect information, including with respect to privacy, confidentiality, or information security, if those obligations would impose greater protection requirements than this title or the amendments made by this title.

(4) **FOIA EXEMPTION.**—Any report received by the Director pursuant to paragraph (1) shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code

(commonly known as the “Freedom of Information Act”).

(b) **CREATION OF COUNCIL.**—Section 1752(c) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)) is amended—

(1) in paragraph (1)—
 (A) in subparagraph (G), by striking “and” at the end;

(B) by redesignating subparagraph (H) as subparagraph (I); and

(C) by inserting after subparagraph (G) the following:

“(H) lead an intergovernmental Cyber Incident Reporting Council, in coordination with the Director of the Office of Management and Budget, the Attorney General, and the Director of the Cybersecurity and Infrastructure Security Agency and in consultation with Sector Risk Management Agencies (as defined in section 2201 of the Homeland Security Act of 2002 (6 U.S.C. 651)) and other appropriate Federal agencies, to coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations, for covered entities (as defined in section 2230 of such Act) and entities that make a ransom payment (as defined in such section 2201 (6 U.S.C. 651)); and”; and

(2) by adding at the end the following:
 “(3) **RULE OF CONSTRUCTION.**—Nothing in paragraph (1)(H) shall be construed to provide any additional regulatory authority to any Federal entity.”.

(c) **HARMONIZING REPORTING REQUIREMENTS.**—The National Cyber Director shall, in consultation with the Director, the Attorney General, the Cyber Incident Reporting Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), and the Director of the Office of Management and Budget, to the maximum extent practicable—

(1) periodically review existing regulatory requirements, including the information required in such reports, to report cyber incidents and ensure that any such reporting requirements and procedures avoid conflicting, duplicative, or burdensome requirements; and

(2) coordinate with the Director, the Attorney General, and regulatory authorities that receive reports relating to cyber incidents to identify opportunities to streamline reporting processes, and where feasible, facilitate interagency agreements between such authorities to permit the sharing of such reports, consistent with applicable law and policy, without impacting the ability of such agencies to gain timely situational awareness of a covered cyber incident or ransom payment.

SEC. 5105. RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.

(a) **PROGRAM.**—Not later than 1 year after the date of enactment of this Act, the Director shall establish a ransomware vulnerability warning program to leverage existing authorities and technology to specifically develop processes and procedures for, and to dedicate resources to, identifying information systems that contain security vulnerabilities associated with common ransomware attacks, and to notify the owners of those vulnerable systems of their security vulnerability.

(b) **IDENTIFICATION OF VULNERABLE SYSTEMS.**—The pilot program established under subsection (a) shall—

(1) identify the most common security vulnerabilities utilized in ransomware attacks and mitigation techniques; and

(2) utilize existing authorities to identify Federal and other relevant information systems that contain the security vulnerabilities identified in paragraph (1).

(c) **ENTITY NOTIFICATION.**—

(1) **IDENTIFICATION.**—If the Director is able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may notify the owner of the information system.

(2) **NO IDENTIFICATION.**—If the Director is not able to identify the entity at risk that owns or operates a vulnerable information system identified in subsection (b), the Director may utilize the subpoena authority pursuant to section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) to identify and notify the entity at risk pursuant to the procedures within that section.

(3) **REQUIRED INFORMATION.**—A notification made under paragraph (1) shall include information on the identified security vulnerability and mitigation techniques.

(d) **PRIORITIZATION OF NOTIFICATIONS.**—To the extent practicable, the Director shall prioritize covered entities for identification and notification activities under the pilot program established under this section.

(e) **LIMITATION ON PROCEDURES.**—No procedure, notification, or other authorities utilized in the execution of the pilot program established under subsection (a) shall require an owner or operator of a vulnerable information system to take any action as a result of a notice of a security vulnerability made pursuant to subsection (c).

(f) **RULE OF CONSTRUCTION.**—Nothing in this section shall be construed to provide additional authorities to the Director to identify vulnerabilities or vulnerable systems.

(g) **TERMINATION.**—The pilot program established under subsection (a) shall terminate on the date that is 4 years after the date of enactment of this Act.

SEC. 5106. RANSOMWARE THREAT MITIGATION ACTIVITIES.

(a) **JOINT RANSOMWARE TASK FORCE.**—
 (1) **IN GENERAL.**—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in consultation with the Attorney General and the Director of the Federal Bureau of Investigation, shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks, and identify and pursue opportunities for international cooperation.

(2) **COMPOSITION.**—The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the National Cyber Director in consultation with the Secretary of Homeland Security.

(3) **RESPONSIBILITIES.**—The Joint Ransomware Task Force, utilizing only existing authorities of each participating agency, shall coordinate across the Federal Government the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with relevant private sector, State, local, Tribal, and territorial governments and international stakeholders to identify needs and establish mechanisms for providing input into the Task Force.

(C) Identifying, in consultation with relevant entities, a list of highest threat ransomware entities updated on an ongoing basis, in order to facilitate—

(i) prioritization for Federal action by appropriate Federal agencies; and

(ii) identify metrics for success of said actions.

(D) Disrupting ransomware criminal actors, associated infrastructure, and their finances.

(E) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(F) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

(G) Creation of after-action reports and other lessons learned from Federal actions that identify successes and failures to improve subsequent actions.

(H) Any other activities determined appropriate by the task force to mitigate the threat of ransomware attacks against Federal and non-Federal entities.

(b) **CLARIFYING PRIVATE SECTOR LAWFUL DEFENSIVE MEASURES.**—Not later than 180 days after the date of enactment of this Act, the National Cyber Director, in coordination with the Secretary of Homeland Security and the Attorney General, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary of the Senate and the Committee on Homeland Security, the Committee on the Judiciary, and the Committee on Oversight and Reform of the House of Representatives a report that describes defensive measures that private sector actors can take when countering ransomware attacks and what laws need to be clarified to enable that action.

(c) **RULE OF CONSTRUCTION.**—Nothing in this section shall be construed to provide any additional authority to any Federal agency.

SEC. 5107. CONGRESSIONAL REPORTING.

(a) **REPORT ON STAKEHOLDER ENGAGEMENT.**—Not later than 30 days after the date on which the Director issues the final rule under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103(b) of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that describes how the Director engaged stakeholders in the development of the final rule.

(b) **REPORT ON OPPORTUNITIES TO STRENGTHEN SECURITY RESEARCH.**—Not later than 1 year after the date of enactment of this Act, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report describing how the National Cybersecurity and Communications Integration Center established under section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) has carried out activities under section 2231(a)(9) of the Homeland Security Act of 2002, as added by section 5103(a) of this title, by proactively identifying opportunities to use cyber incident data to inform and enable cybersecurity research within the academic and private sector.

(c) **REPORT ON RANSOMWARE VULNERABILITY WARNING PILOT PROGRAM.**—Not later than 1 year after the date of enactment of this Act, and annually thereafter for the duration of the pilot program established under section 5105, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report, which may include a classified annex, on the effectiveness of the pilot program, which shall include a discussion of the following:

(1) The effectiveness of the notifications under section 5105(c) in mitigating security vulnerabilities and the threat of ransomware.

(2) Identification of the most common vulnerabilities utilized in ransomware.

(3) The number of notifications issued during the preceding year.

(4) To the extent practicable, the number of vulnerable devices or systems mitigated

under this pilot by the Agency during the preceding year.

(d) **REPORT ON HARMONIZATION OF REPORTING REGULATIONS.**—

(1) **IN GENERAL.**—Not later than 180 days after the date on which the National Cyber Director convenes the Council described in section 1752(c)(1)(H) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 1500(c)(1)(H)), the National Cyber Director shall submit to the appropriate congressional committees a report that includes—

(A) a list of duplicative Federal cyber incident reporting requirements on covered entities and entities that make a ransom payment;

(B) a description of any challenges in harmonizing the duplicative reporting requirements;

(C) any actions the National Cyber Director intends to take to facilitate harmonizing the duplicative reporting requirements; and

(D) any proposed legislative changes necessary to address the duplicative reporting.

(2) **RULE OF CONSTRUCTION.**—Nothing in paragraph (1) shall be construed to provide any additional regulatory authority to any Federal agency.

(e) **GAO REPORTS.**—

(1) **IMPLEMENTATION OF THIS TITLE.**—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the implementation of this title and the amendments made by this title.

(2) **EXEMPTIONS TO REPORTING.**—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103 of this title, the Comptroller General of the United States shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the exemptions to reporting under paragraphs (2) and (5) of section 2232(a) of the Homeland Security Act of 2002, as added by section 5103 of this title, which shall include—

(A) to the extent practicable, an evaluation of the quantity of incidents not reported to the Federal Government;

(B) an evaluation of the impact on impacted entities, homeland security, and the national economy of the ransomware criminal ecosystem of incidents and ransom payments, including a discussion on the scope of impact of incidents that were not reported to the Federal Government;

(C) an evaluation of the burden, financial and otherwise, on entities required to report cyber incidents under this title, including an analysis of entities that meet the definition of a small organization and would be exempt from ransom payment reporting but not for being a covered entity; and

(D) a description of the consequences and effects of the exemptions.

(f) **REPORT ON EFFECTIVENESS OF ENFORCEMENT MECHANISMS.**—Not later than 1 year after the date on which the Director issues the final rule required under section 2232(b) of the Homeland Security Act of 2002, as added by section 5103 of this title, the Director shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the effectiveness of the enforcement mechanisms within section 2234 of the Homeland Security Act of 2002, as added by section 5103 of this title.

TITLE LI—CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS ACT OF 2021

SEC. 5201. SHORT TITLE.

This title may be cited as the “CISA Technical Corrections and Improvements Act of 2021”.

SEC. 5202. REDESIGNATIONS.

(a) **IN GENERAL.**—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217; and

(5) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216.

(b) **TECHNICAL AND CONFORMING AMENDMENTS.**—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in paragraph (11), by striking “and” at the end;

(2) in the first paragraph (12)—

(A) by striking “section 2215” and inserting “section 2217”; and

(B) by striking “and” at the end; and

(3) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) **ADDITIONAL TECHNICAL AMENDMENT.**—

(1) **AMENDMENT.**—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116-260) is amended, in the matter preceding subparagraph (A), by striking “Homeland Security Act” and inserting “Homeland Security Act of 2002”.

(2) **EFFECTIVE DATE.**—The amendment made by paragraph (1) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116-260).

SEC. 5203. CONSOLIDATION OF DEFINITIONS.

(a) **IN GENERAL.**—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitle A heading the following:

“SEC. 2200. DEFINITIONS.

“Except as otherwise specifically provided, in this title:

“(1) **AGENCY.**—The term ‘Agency’ means the Cybersecurity and Infrastructure Security Agency.

“(2) **AGENCY INFORMATION.**—The term ‘agency information’ means information collected or maintained by or on behalf of an agency.

“(3) **AGENCY INFORMATION SYSTEM.**—The term ‘agency information system’ means an information system used or operated by an agency or by another entity on behalf of an agency.

“(4) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term ‘appropriate congressional committees’ means—

“(A) the Committee on Homeland Security and Governmental Affairs of the Senate; and

“(B) the Committee on Homeland Security of the House of Representatives.

“(5) **CLOUD SERVICE PROVIDER.**—The term ‘cloud service provider’ means an entity offering products or services related to cloud computing, as defined by the National Institutes of Standards and Technology in NIST Special Publication 800-145 and any amendatory or superseding document relating thereto.

“(6) **CRITICAL INFRASTRUCTURE INFORMATION.**—The term ‘critical infrastructure information’ means information not customarily in the public domain and related to the security of critical infrastructure or protected systems, including—

“(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

“(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

“(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

“(7) CYBER THREAT INDICATOR.—The term ‘cyber threat indicator’ means information that is necessary to describe or identify—

“(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

“(B) a method of defeating a security control or exploitation of a security vulnerability;

“(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

“(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

“(E) malicious cyber command and control;

“(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

“(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

“(H) any combination thereof.

“(8) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

“(9) CYBERSECURITY RISK.—The term ‘cybersecurity risk’—

“(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

“(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

“(10) CYBERSECURITY THREAT.—

“(A) IN GENERAL.—Except as provided in subparagraph (B), the term ‘cybersecurity threat’ means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that

is stored on, processed by, or transiting an information system.

“(B) EXCLUSION.—The term ‘cybersecurity threat’ does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

“(11) DEFENSIVE MEASURE.—

“(A) IN GENERAL.—Except as provided in subparagraph (B), the term ‘defensive measure’ means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

“(B) EXCLUSION.—The term ‘defensive measure’ does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

“(i) the entity operating the measure; or

“(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

“(12) HOMELAND SECURITY ENTERPRISE.—The term ‘Homeland Security Enterprise’ means relevant governmental and non-governmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

“(13) INCIDENT.—The term ‘incident’ means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

“(14) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ‘Information Sharing and Analysis Organization’ means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

“(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

“(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

“(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

“(15) INFORMATION SYSTEM.—The term ‘information system’ has the meaning given the term in section 3502 of title 44, United States Code.

“(16) INTELLIGENCE COMMUNITY.—The term ‘intelligence community’ has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

“(17) MANAGED SERVICE PROVIDER.—The term ‘managed service provider’ means an entity that delivers services, such as network, application, infrastructure, or security services, via ongoing and regular support and active administration on the premises of a customer, in the data center of the entity

(such as hosting), or in a third party data center.

“(18) MONITOR.—The term ‘monitor’ means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

“(19) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term ‘national cybersecurity asset response activities’ means—

“(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

“(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

“(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

“(D) facilitating information sharing and operational coordination with threat response; and

“(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

“(20) NATIONAL SECURITY SYSTEM.—The term ‘national security system’ has the meaning given the term in section 11103 of title 40, United States Code.

“(21) RANSOM PAYMENT.—The term ‘ransom payment’ means the transmission of any money or other property or asset, including virtual currency, or any portion thereof, which has at any time been delivered as ransom in connection with a ransomware attack.

“(22) RANSOMWARE ATTACK.—The term ‘ransomware attack’—

“(A) means a cyber incident that includes the use or threat of use of unauthorized or malicious code on an information system, or the use or threat of use of another digital mechanism such as a denial of service attack, to interrupt or disrupt the operations of an information system or compromise the confidentiality, availability, or integrity of electronic data stored on, processed by, or transiting an information system to extort a demand for a ransom payment; and

“(B) does not include any such event where the demand for payment is made by a Federal Government entity, good faith security research, or in response to an invitation by the owner or operator of the information system for third parties to identify vulnerabilities in the information system.

“(23) SECTOR RISK MANAGEMENT AGENCY.—The term ‘Sector Risk Management Agency’ means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

“(24) SECURITY CONTROL.—The term ‘security control’ means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

“(25) SECURITY VULNERABILITY.—The term ‘security vulnerability’ means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

“(26) SHARING.—The term ‘sharing’ (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).

“(27) SUPPLY CHAIN COMPROMISE.—The term ‘supply chain compromise’ means a cyber incident within the supply chain of an information system that an adversary can leverage to jeopardize the confidentiality, integrity, or availability of the information technology system or the information the system processes, stores, or transmits, and can occur at any point during the life cycle.”

“(28) VIRTUAL CURRENCY.—The term ‘virtual currency’ means the digital representation of value that functions as a medium of exchange, a unit of account, or a store of value.”

“(29) VIRTUAL CURRENCY ADDRESS.—The term ‘virtual currency address’ means a unique public cryptographic key identifying the location to which a virtual currency payment can be made.”

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

“SEC. 2201. DEFINITION.

“In this subtitle, the term ‘Cybersecurity Advisory Committee’ means the advisory committee established under section 2219(a).”;

(2) in section 2202—

(A) in subsection (a)(1), by striking “(in this subtitle referred to as the Agency)”;

(B) in subsection (f)—

(i) in paragraph (1), by inserting “Executive” before “Assistant Director”; and

(ii) in paragraph (2), by inserting “Executive” before “Assistant Director”;

(3) in section 2203(a)(2), by striking “as the ‘Assistant Director’” and inserting “as the ‘Executive Assistant Director’”;

(4) in section 2204(a)(2), by striking “as the ‘Assistant Director’” and inserting “as the ‘Executive Assistant Director’”;

(5) in section 2209—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)—

(i) in subparagraph (A)(iii), as so redesignated, by striking “, as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))”; and

(ii) in subparagraph (B)(ii), by striking “information sharing and analysis organizations” and inserting “Information Sharing and Analysis Organizations”;

(D) in subsection (d), as so redesignated—

(i) in the matter preceding paragraph (1), by striking “subsection (c)” and inserting “subsection (b)”;

(ii) in paragraph (1)(E)(ii)(II), by striking “information sharing and analysis organizations” and inserting “Information Sharing and Analysis Organizations”;

(E) in subsection (j), as so redesignated, by striking “subsection (c)(8)” and inserting “subsection (b)(8)”;

(F) in subsection (n), as so redesignated—

(i) in paragraph (2)(A), by striking “subsection (c)(12)” and inserting “subsection (b)(12)”;

(ii) in paragraph (3)(B)(i), by striking “subsection (c)(12)” and inserting “subsection (b)(12)”;

(6) in section 2210—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(C) in subsection (b), as so redesignated—

(i) by striking “information sharing and analysis organizations (as defined in section 2222(5))” and inserting “Information Sharing and Analysis Organizations”; and

(ii) by striking “(as defined in section 2209)”;

(D) in subsection (c), as so redesignated, by striking “subsection (c)” and inserting “subsection (b)”;

(7) in section 2211, by striking subsection (h);

(8) in section 2212, by striking “information sharing and analysis organizations (as defined in section 2222(5))” and inserting “Information Sharing and Analysis Organizations”;

(9) in section 2213—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (f) as subsections (a) through (e); respectively;

(C) in subsection (b), as so redesignated, by striking “subsection (b)” each place it appears and inserting “subsection (a)”;

(D) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking “subsection (b)” and inserting “subsection (a)”;

(E) in subsection (d), as so redesignated—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking “subsection (c)(2)” and inserting “subsection (b)(2)”;

(II) in subparagraph (A), by striking “subsection (c)(1)” and inserting “subsection (b)(1)”;

(III) in subparagraph (B), by striking “subsection (c)(2)” and inserting “subsection (b)(2)”;

(ii) in paragraph (2), by striking “subsection (c)(2)” and inserting “subsection (b)(2)”;

(10) in section 2216, as so redesignated—

(A) in subsection (d)(2), by striking “information sharing and analysis organizations” and inserting “Information Sharing and Analysis Organizations”; and

(B) by striking subsection (f) and inserting the following:

“(f) CYBER DEFENSE OPERATION DEFINED.—In this section, the term ‘cyber defense operation’ means the use of a defensive measure.”;

(11) in section 2218(c)(4)(A), as so redesignated, by striking “information sharing and analysis organizations” and inserting “Information Sharing and Analysis Organizations”;

(12) in section 2222—

(A) by striking paragraphs (3), (5), and (8);

(B) by redesignating paragraph (4) as paragraph (3); and

(C) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXII the following:

“Sec. 2200. Definitions.”;

(2) by striking the item relating to section 2201 and inserting the following:

“Sec. 2201. Definition.”; and

(3) by striking the item relating to section 2214 and all that follows through the item relating to section 2217 and inserting the following:

“Sec. 2214. National Asset Database.

“Sec. 2215. Duties and authorities relating to .gov internet domain.

“Sec. 2216. Joint Cyber Planning Office.

“Sec. 2217. Cybersecurity State Coordinator.

“Sec. 2218. Sector Risk Management Agencies.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity Education and Training Programs.”.

(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

“(4) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(5) CYBERSECURITY THREAT.—The term ‘cybersecurity threat’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(6) CYBER THREAT INDICATOR.—The term ‘cyber threat indicator’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(7) DEFENSIVE MEASURE.—The term ‘defensive measure’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”;

(2) by striking paragraph (13) and inserting the following:

“(13) MONITOR.—The term ‘monitor’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”; and

(3) by striking paragraphs (16) and (17) and inserting the following:

“(16) SECURITY CONTROL.—The term ‘security control’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

“(17) SECURITY VULNERABILITY.—The term ‘security vulnerability’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”.

SEC. 5204. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking “section 2210” and inserting “section 2200”; and

(B) in paragraph (4), by striking “section 2209” and inserting “section 2200”;

(2) in section 223(b) (6 U.S.C. 151 note), by striking “section 2213(b)(1)” each place it appears and inserting “section 2213(a)(1)”;

(3) in section 226 (6 U.S.C. 1524)—

(A) in subsection (a)—

(i) in paragraph (1), by striking “section 2213” and inserting “section 2200”;

(ii) in paragraph (2), by striking “section 102” and inserting “section 2200 of the Homeland Security Act of 2002”;

(iii) in paragraph (4), by striking “section 2210(b)(1)” and inserting “section 2210(a)(1)”;

(iv) in paragraph (5), by striking “section 2213(b)” and inserting “section 2213(a)”;

(B) in subsection (c)(1)(A)(vi), by striking “section 2213(c)(5)” and inserting “section 2213(b)(5)”;

(4) in section 227(b) (6 U.S.C. 1525(b)), by striking “section 2213(d)(2)” and inserting “section 2213(c)(2)”.

(b) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking “section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))” and inserting “section 2210(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))”.

(c) WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking “section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))” and inserting “section 2200 of the Homeland Security Act of 2002”; and

(B) by amending paragraph (7) to read as follows:

“(7) SECTOR RISK MANAGEMENT AGENCY.—The term ‘Sector Risk Management Agency’ has the meaning given the term in section 2200 of the Homeland Security Act of 2002.”;

(2) in subsection (c)(3)(B), by striking “section 2201(5)” and inserting “section 2200”; and

(3) in subsection (d)—

(A) by striking “section 2215” and inserting “section 2218”; and

(B) by striking “, as added by this section”.

(d) NATIONAL SECURITY ACT OF 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking “section 226 of the Homeland Security Act of 2002 (6 U.S.C. 147)” and inserting “section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)”.

(e) IoT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking “section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))” and inserting “section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(l))”.

(f) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of the Small Business Act (15 U.S.C. 648(a)(8)(B)) is amended by striking “section 2209(a)” and inserting “section 2200”.

(g) TITLE 46.—Section 70101(2) of title 46, United States Code, is amended by striking “section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)” and inserting “section 2200 of the Homeland Security Act of 2002”.

SA 4674. Mr. PETERS (for himself and Mr. PORTMAN) submitted an amendment intended to be proposed to amendment SA 3867 submitted by Mr. REED and intended to be proposed to the bill H.R. 4350, to authorize appropriations for fiscal year 2022 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end, add the following:

DIVISION E—FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2021

SEC. 5101. SHORT TITLE.

This division may be cited as the “Federal Information Security Modernization Act of 2021”.

SEC. 5102. DEFINITIONS.

In this division, unless otherwise specified:

(1) **ADDITIONAL CYBERSECURITY PROCEDURE.**—The term “additional cybersecurity procedure” has the meaning given the term in section 3552(b) of title 44, United States Code, as amended by this division.

(2) **AGENCY.**—The term “agency” has the meaning given the term in section 3502 of title 44, United States Code.

(3) **APPROPRIATE CONGRESSIONAL COMMITTEES.**—The term “appropriate congressional committees” means—

(A) the Committee on Homeland Security and Governmental Affairs of the Senate;

(B) the Committee on Oversight and Reform of the House of Representatives; and

(C) the Committee on Homeland Security of the House of Representatives.

(4) **DIRECTOR.**—The term “Director” means the Director of the Office of Management and Budget.

(5) **INCIDENT.**—The term “incident” has the meaning given the term in section 3552(b) of title 44, United States Code.

(6) **NATIONAL SECURITY SYSTEM.**—The term “national security system” has the meaning given the term in section 3552(b) of title 44, United States Code.

(7) **PENETRATION TEST.**—The term “penetration test” has the meaning given the term in

section 3552(b) of title 44, United States Code, as amended by this division.

(8) **THREAT HUNTING.**—The term “threat hunting” means proactively and iteratively searching for threats to systems that evade detection by automated threat detection systems.

TITLE LI—UPDATES TO FISMA

SEC. 5121. TITLE 44 AMENDMENTS.

(a) **SUBCHAPTER I AMENDMENTS.**—Subchapter I of chapter 35 of title 44, United States Code, is amended—

(1) in section 3504—

(A) in subsection (a)(1)(B)—

(i) by striking clause (v) and inserting the following:

“(v) confidentiality, privacy, disclosure, and sharing of information;”;

(ii) by redesignating clause (vi) as clause (vii); and

(iii) by inserting after clause (v) the following:

“(vi) in consultation with the National Cyber Director and the Director of the Cybersecurity and Infrastructure Security Agency, security of information; and”;

(B) in subsection (g), by striking paragraph (1) and inserting the following:

“(1) develop, and in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the National Cyber Director, oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies; and”;

(2) in section 3505—

(A) in paragraph (3) of the first subsection designated as subsection (c)—

(i) in subparagraph (B)—

(I) by inserting “the Director of the Cybersecurity and Infrastructure Security Agency, the National Cyber Director, and” before “the Comptroller General”; and

(II) by striking “and” at the end;

(ii) in subparagraph (C)(v), by striking the period at the end and inserting “; and”; and

(iii) by adding at the end the following:

“(D) maintained on a continual basis through the use of automation, machine-readable data, and scanning.”;

(B) by striking the second subsection designated as subsection (c);

(3) in section 3506—

(A) in subsection (b)(1)(C), by inserting “, availability” after “integrity”; and

(B) in subsection (h)(3), by inserting “security,” after “efficiency.”;

(4) in section 3513—

(A) by redesignating subsection (c) as subsection (d); and

(B) by inserting after subsection (b) the following:

“(c) Each agency providing a written plan under subsection (b) shall provide any portion of the written plan addressing information security or cybersecurity to the Director of the Cybersecurity and Infrastructure Security Agency.”.

(b) **SUBCHAPTER II DEFINITIONS.**—

(1) **IN GENERAL.**—Section 3552(b) of title 44, United States Code, is amended—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), (6), and (7) as paragraphs (2), (3), (4), (5), (6), (9), and (11), respectively;

(B) by inserting before paragraph (2), as so redesignated, the following:

“(1) The term ‘additional cybersecurity procedure’ means a process, procedure, or other activity that is established in excess of the information security standards promulgated under section 11331(b) of title 40 to increase the security and reduce the cybersecurity risk of agency systems.”;

(C) by inserting after paragraph (6), as so redesignated, the following:

“(7) The term ‘high value asset’ means information or an information system that the head of an agency determines so critical to the agency that the loss or corruption of the information or the loss of access to the information system would have a serious impact on the ability of the agency to perform the mission of the agency or conduct business.

“(8) The term ‘major incident’ has the meaning given the term in guidance issued by the Director under section 3598(a).”;

(D) by inserting after paragraph (9), as so redesignated, the following:

“(10) The term ‘penetration test’ means a specialized type of assessment that—

“(A) is conducted on an information system or a component of an information system; and

“(B) emulates an attack or other exploitation capability of a potential adversary, typically under specific constraints, in order to identify any vulnerabilities of an information system or a component of an information system that could be exploited.”;

(E) by inserting after paragraph (11), as so redesignated, the following:

“(12) The term ‘shared service’ means a centralized business or mission capability that is provided to multiple organizations within an agency or to multiple agencies.”.

(2) CONFORMING AMENDMENTS.—

(A) **HOMELAND SECURITY ACT OF 2002.**—Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(1)(A)) is amended by striking “section 3552(b)(5)” and inserting “section 3552(b)”.

(B) **TITLE 10.—**

(i) **SECTION 2222.**—Section 2222(i)(8) of title 10, United States Code, is amended by striking “section 3552(b)(6)(A)” and inserting “section 3552(b)(9)(A)”.

(ii) **SECTION 2223.**—Section 2223(c)(3) of title 10, United States Code, is amended by striking “section 3552(b)(6)” and inserting “section 3552(b)”.

(iii) **SECTION 2315.**—Section 2315 of title 10, United States Code, is amended by striking “section 3552(b)(6)” and inserting “section 3552(b)”.

(iv) **SECTION 2339A.**—Section 2339a(e)(5) of title 10, United States Code, is amended by striking “section 3552(b)(6)” and inserting “section 3552(b)”.

(C) **HIGH-PERFORMANCE COMPUTING ACT OF 1991.**—Section 207(a) of the High-Performance Computing Act of 1991 (15 U.S.C. 5527(a)) is amended by striking “section 3552(b)(6)(A)(i)” and inserting “section 3552(b)(9)(A)(i)”.

(D) **INTERNET OF THINGS CYBERSECURITY IMPROVEMENT ACT OF 2020.**—Section 3(5) of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3a) is amended by striking “section 3552(b)(6)” and inserting “section 3552(b)”.

(E) **NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013.**—Section 933(e)(1)(B) of the National Defense Authorization Act for Fiscal Year 2013 (10 U.S.C. 2224 note) is amended by striking “section 3542(b)(2)” and inserting “section 3552(b)”.

(F) **IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011.**—The Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383) is amended—

(i) in section 806(e)(5) (10 U.S.C. 2304 note), by striking “section 3542(b)” and inserting “section 3552(b)”;

(ii) in section 931(b)(3) (10 U.S.C. 2223 note), by striking “section 3542(b)(2)” and inserting “section 3552(b)”;

(iii) in section 932(b)(2) (10 U.S.C. 2224 note), by striking “section 3542(b)(2)” and inserting “section 3552(b)”.

(G) **E-GOVERNMENT ACT OF 2002.**—Section 301(c)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended by striking